Тема 2.3. Инженерно-технические мероприятия по обеспечению антитеррористической защищенности.

Основными причинами, способствующими террористической уязвимости объектов (территорий), является наличие потенциально опасных участков и критических элементов объекта, в отношении которых не выполняются или выполняются не в полной мере требования к их антитеррористической защищенности. Устранение этих причин обеспечивается в том числе путем реализации инженерно-технических мер.

Инженерная защита объектов (территорий) осуществляется в соответствии с Федеральным законом «Технический регламент о безопасности зданий и сооружений». Выбор и оснащение объектов (территорий) инженерно-техническими средствами и системами охраны конкретных типов определяются в техническом задании на проектирование инженерно-технических средств охраны при новом строительстве, капитальном ремонте, реконструкции или модернизации объектов (территорий).
Методологической основой для обеспечения инженерно-технических основ антитеррористической защищенности выступают разработанные в 2022 году Росгвардией **рекомендации** по оборудованию инженерно-техническими средствами охраны социально значимых объектов (территорий), находящихся в сфере деятельности Минобрнауки России и Минпросвещения России.

На большинство инженерно-технических мероприятий существуют ГОСТы, регламентирующие состав и принципы построения, технические характеристики. Выбор конкретных типов и моделей оборудования и материалов зависит от реальной необходимости, бюджета, немаловажным фактором, в зависимости от количества объектов, является унификация решений и возможность объединения систем, намного удобнее контролировать работоспособность и проводить мониторинг из-под единой оболочки.

Реализация всех вышеперечисленных мероприятий по антитеррористической защищенности возможна только в случае грамотного взаимодействия служб и подразделений образовательной организации. В первую очередь, это касается организации и обеспечения пропускного и внутриобъектового режимов, контроля за их функционированием, а также оснащения объектов (территорий) инженерно-техническими средствами и системами охраны и (или) обеспечения охраны объектов (территорий) охранными организациями. **Согласно Постановлению № 1421**, для обеспечения антитеррористической защищенности объектов (территорий) **независимо от категории** опасности, подведомственных Минобрнауки России, необходимо:

- инженерно-техническое обеспечение пропускного и внутриобъектового режимов и контроля за их функционированием;
- оснащение объектов (территорий) инженерно-техническими средствами и системами охраны (в том числе системами передачи тревожных сообщений в подразделения войск национальной гвардии Российской Федерации или в систему обеспечения вызова экстренных оперативных служб по единому номеру "112") и поддержание их в исправном состоянии, оснащение объектов (территорий) бесперебойной и устойчивой связью;

– организация круглосуточной охраны, ежедневная проверка (обход и осмотр) зданий (строений, сооружений), потенциально опасных участков и критических элементов объекта (территории), стоянок автотранспорта, складских и подсобных помещений;

– исключение бесконтрольного пребывания на объекте (территории) посторонних лиц и нахождения транспортных средств, а также в непосредственной близости от объекта (территории);

– оборудование объектов (территорий) системами экстренного оповещения работников, обучающихся и иных лиц, находящихся на объекте (территории), о потенциальной угрозе возникновения или возникновении чрезвычайной ситуации;

– осуществление мероприятий информационной безопасности, обеспечивающих защиту от несанкционированного доступа к информационным ресурсам объектов (территорий).

Если необходимо обеспечить антитеррористическую защищенность объектов (территорий) **второй категории**, то помимо указанных ранее действий следует провести мероприятия по:

– обеспечению охраны объектов (территорий) с использованием соответствующего оборудования работниками частных охранных организаций, или подразделениями ведомственной охраны федеральных органов исполнительной власти, имеющих право на создание ведомственной охраны, или подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации, или военизированными и сторожевыми подразделениями организации, подведомственной Федеральной службе войск национальной гвардии Российской Федерации;

– оборудованию объектов (территорий) инженерно-техническими средствами и системами охраны (системой видеонаблюдения, контроля и управления доступом, охранной сигнализацией).

К антитеррористической защищенности объектов (территорий**) первой категории** с инженерно-технической точки зрения помимо всех ранее обозначенных применяются еще более жесткие требования:

– оборудование потенциально опасных участков и критических элементов объекта (территории) системой видеонаблюдения, обеспечивающей передачу визуальной информации о состоянии периметра потенциально опасных участков и мест доступа к критическим элементам объекта (территории);

– оборудование контрольно-пропускных пунктов и въездов на объект (территорию) системами видеонаблюдения, обеспечивающими круглосуточную видеофиксацию, с зонами обзора видеокамер, позволяющими осуществлять идентификацию и (или) различение (распознавание);

– оснащение въездов на объект (территорию) воротами, обеспечивающими жесткую фиксацию их створок в закрытом положении, а также при необходимости средствами снижения скорости и (или) противотаранными устройствами.

Согласно Постановлению № 1421, для обеспечения антитеррористической защищенности объектов (территорий) в целях обеспечения антитеррористической защищенности объектов (территорий), **отнесенных к четвертой категории опасности**, осуществляются следующие мероприятия:

- оснащение объектов (территорий) системами передачи тревожных сообщений в подразделения войск национальной гвардии Российской Федерации или в систему обеспечения вызова экстренных оперативных служб по единому номеру "112" и поддержание их в исправном состоянии;

- оборудование объектов (территорий) системами оповещения и управления эвакуацией либо автономными системами (средствами) экстренного оповещения работников, обучающихся и иных лиц, находящихся на объекте (территории), о потенциальной угрозе возникновения или о возникновении чрезвычайной ситуации;

- исключение бесконтрольного пребывания на объекте (территории) посторонних лиц и нахождения транспортных средств, в том числе в непосредственной близости от объекта (территории);

- оснащение объектов (территорий) системой наружного освещения;

В отношении объектов (территорий) **третьей категории опасности** дополнительно к мероприятиям, предусмотренным пунктом 24 настоящих требований, осуществляются следующие мероприятия:

- оснащение объектов (территорий) системами видеонаблюдения, охранной сигнализации;

- оборудование на 1-м этаже помещения для охраны с установкой в нем систем видеонаблюдения, охранной сигнализации и средств передачи тревожных сообщений в подразделения войск национальной гвардии Российской Федерации (подразделения вневедомственной охраны войск национальной гвардии Российской Федерации);

- оборудование основных входов в здания, входящие в состав объектов (территорий), контрольно-пропускными пунктами (постами охраны);

- оснащение объектов (территорий) стационарными или ручными металлоискателями.

В отношении объектов (территорий) **второй категории опасности** дополнительно к мероприятиям, предусмотренным пунктами 24 и 25 настоящих требований, осуществляются следующие мероприятия:

- оборудование объектов (территорий) системой контроля и управления доступом;

- оснащение въездов на объект (территорию) воротами, обеспечивающими жесткую фиксацию их створок в закрытом положении.

В отношении объектов (территорий) **первой категории опасности** дополнительно к мероприятиям, предусмотренным пунктами 24, 25 и 26 настоящих требований, осуществляются следующие мероприятия:

- оборудование контрольно-пропускных пунктов при входе (въезде) на прилегающую территорию объекта (территории);

- оснащение въездов на объект (территорию) средствами снижения скорости и (или) противотаранными устройствами.

По решению руководителей органов (организаций), являющихся правообладателями объектов (территорий), объекты (территории) могут оборудоваться инженерно-техническими средствами охраны более высокого класса защиты.

Система видеонаблюдения с учетом количества устанавливаемых камер и мест их размещения должна обеспечивать непрерывный визуальный контроль уязвимых мест и критических элементов объекта (территории), архивирование и хранение данных в течение одного месяца. Система оповещения и управления эвакуацией людей на объекте (территории) должна обеспечивать оперативное информирование лиц, находящихся на объекте (территории), о необходимости эвакуации и других действиях, обеспечивающих безопасность людей, и предотвращение паники. Системы оповещения и управления эвакуацией людей должны быть автономными и оборудованы источниками бесперебойного электропитания. В любой точке объекта (территории), где требуется оповещение людей, уровень громкости, формируемый звуковыми и речевыми оповещателями, должен быть выше допустимого уровня шума. Речевые оповещатели должны быть расположены таким образом, чтобы в любой точке объекта (территории), где требуется оповещение людей, обеспечивалась разборчивость передаваемой речевой информации.

Ограждение территории.

В явном виде в Постановлениях нигде нет требования к ограждению территории, кроме характеристики в форме паспорта безопасности. Однако для силовиков ограждение территории является обязательным для исполнения требования исключения бесконтрольного пребывания на объекте (территории) посторонних лиц и нахождения транспортных средств, а также в непосредственной близости от объекта (территории). Требования к ограждению для объектов и территорий должны соответствовать ГОСТ Р 57278-2016:

Ограждение периметра объекта рекомендуется выполнять преимущественно в виде прямолинейных участков с минимальным количеством изгибов и поворотов, что обеспечит наиболее благоприятные условия для функционирования периметровых технических средств обнаружения проникновения и осуществления визуального наблюдения за периметром, в том числе с применением СОТ.

Ограждение не должно иметь повреждений, конструктивных элементов, которые можно использовать в качестве лазов, а также незапираемых дверей, ворот и калиток.

К ограждению не должны примыкать какие-либо пристройки, кроме зданий, являющихся составной частью периметра.

Социально значимые объекты (территории) Министерства науки и высшего образования Российской Федерации рекомендуется оборудовать ограждением высотой порядка 2,5 м, а в районах с глубиной снежного покрова более одного метра – порядка 3 м.

Основное ограждение может быть просматриваемым или глухим, иметь сплошное или секционное, жесткое или гибкое полотно.

Для повышения сложности преодоления основного ограждения методом перелезания оно может быть оснащено дополнительным верхним

ограждением.
Дополнительное верхнее ограждение может быть выполнено в виде сварных сетчатых панелей.
Тип и размер опор выбирается исходя из типа выбранного материала и конструкции полотна ограждения.
Главным требованием при этом является способность материала и типа опор удерживать полотно ограждения при значительных внешних воздействиях и обеспечить охранные функции ограждения.
Основное ограждение может устанавливаться на ленточный железобетонный фундамент высотой над уровнем грунта порядка 0,5 м или на свайный фундамент. 14
При установке на свайный фундамент основное ограждение рекомендуется оборудовать дополнительным нижним ограждением.
Дополнительное нижнее ограждение применяется для повышения сложности преодоления основного ограждения методами пролаза или подкопа под полотном ограждения между сваями.
При необходимости установки нижнего дополнительного ограждения для защиты от подкопа, оно должно быть установлено под основным ограждением с заглублением в грунт порядка 0,5 м и выполнено в виде бетонированного цоколя или сварной решетки, изготовленной из стальных прутков диаметром порядка 16 мм, сваренных в пересечениях с ячейкой порядка 150×150 мм.
При необходимости, в соответствии с архитектурноконструктивными решениями данных территорий допускается в качестве основного ограждения использовать ограждения (оговаривается в акте обследования, техническом задании на проектирование):
железобетонное, толщиной порядка 100 мм;
каменное или кирпичное, толщиной порядка 250 мм;
сплошное металлическое с толщиной листа порядка 2 мм, усиленное ребрами жесткости, установленное на ленточный железобетонный фундамент высотой над уровнем грунта порядка 0,5 м, с заглублением в грунт порядка 0,5 м;
декоративные ограждения, изготовленные в виде сварной металлической рамы с заполнением из трубы сечением порядка 25×25 мм, толщиной стенки трубы сечением порядка 3 мм.

Системы передачи тревожных сообщений в подразделения войск национальной гвардии Российской Федерации.

Для обеспечения передачи тревожного сигнала при возникновении опасности необходимо предусмотреть для каждого объекта минимум две тревожных кнопки: стационарная на посту охраны и мобильная (носимая) кнопка либо у охранника, либо у ответственного лица.

Выбор оборудования для передачи тревожного сигнала осуществляется в соответствии со Списком технических средств безопасности, удовлетворяющих «Единым требованиям к системам передачи извещений и объектовым техническим средствам охраны,

предназначенным для применения в подразделениях вневедомственной охраны войск национальной гвардии Российской Федерации» (рекомендован решением расширенного заседания Технического совета ГУВО Росгвардии Протокол №3 от 27 октября 2017 года). Самый простой способ не запутаться в прочтении этого достаточно объемного (64 страницы) документа – обратиться в управление вневедомственной охраны, где технические специалисты или специалисты ПЦО точно скажут, с каким оборудованием может работать ПЦО.

Системы оповещения и управления эвакуацией при террористической угрозе.

Достаточно сложная в исполнении система. До внесения изменений в Постановление Правительства № 1421 пункт про СОЭУ при террористической угрозе звучал следующим образом: Система оповещения является автономной, не совмещенной с ретрансляционными технологическими системами, позволяет осуществлять оперативное информирование лиц, находящихся на объектах Министерства науки и высшего образования Российской Федерации, об актуальных чрезвычайных ситуациях и разновидностях террористических проявлений, поскольку от конкретной ситуации зависит и алгоритм дальнейших действий находящихся на таких объектах лиц (например, безопасная эвакуация либо противодействие преступным
В соответствии с такой формулировкой в Рекомендациях сделан вывод о недопустимости использования в качестве СОУЭ при ТУ СОУЭ при пожаре, для которой приоритетным является информирование о пожаре. При этом технологические требования к СОУЭ при ТУ в точности повторяют требования из ГОСТа к СОЭУ при пожаре.

Сейчас из Постановления исключена несовмещённость с ретрансляционными технологическими системами. Кроме того, требованиями к противопожарной автоматике допускается использование СОУЭ в ручном режиме или автоматическими сценариями, но оповещение при пожаре является приоритетным.

Т.е. в итоге складывается следующая картина: СОУЭ при пожаре использовать нельзя, потому что это написано в Рекомендациях, иных запрещающих документов нет.

Технически оснащение объектов СОУЭ в соответствии с требованиями тоже выглядит достаточно непонятно. Две системы, созданные для сходных задач, на объекте монтируются параллельно, с абсолютно одинаковыми требованиями к размещению оповещателей, громкости оповещения. Если предположить, что одновременно сработают обе системы, мало того, что они будут выдавать противоречащую друг другу информацию, человек, оказавшийся в зоне действия обеих систем физически не сможет понять, что за сообщение транслируется.

Немного о технологических схемах оповещения. Для определения правильности проведения эвакуации весь объект или территория делится на отдельные зоны, для которых проверяются все возможные модели угроз. При необходимости, количество зон в соответствии с моделями может изменяться в любую сторону. Для каждой модели угрозы в зависимости от зоны разрабатывается отдельный сценарий, в соответствии с которым будут заданы пути, маршруты эвакуации или иные решения для персонала и обучающихся. Пример: появление вооруженного человека у центрального входа, обнаружение

подозрительного предмета на входе, в общем, любая ситуация на входной группе. В этом случае разработанный сценарий оповещения должен предусматривать информирование в зонах таким образом, чтобы люди из зоны, содержащей центральный вход, могли эвакуироваться в направлении, исключающем прохождение через входную группу, через другие эвакуационные выходы. Если ситуация требует наоборот оставаться на местах (вооруженный человек уже в здании), то это условие также распространяется на ту зону, в которой развивается ситуация, и при эвакуации персонал и студенты других зон никаким образом не должны проходить через зону происшествия. Таким образом, деление объекта на зоны и формирование сценариев для автоматики – достаточно творческий процесс. Необходимо представить все возможные ситуации во всех возможных вариантах. Для оповещения в ручном режиме необходимо предусматривать консоли с микрофонами. Как правило, консоль управления эвакуацией расположена на посту охраны, и в обязанности охранника входит в том числе организация эвакуации. Решение не совсем корректное с точки зрения АТЗ, охранник чаще всего первым попадает под действие угрозы. Правильным будет назначение ответственного лица за управление эвакуацией, размещение его рабочего места отдельно от поста охраны, оснащение рабочего места системами, дублирующими информацию СВН, ОС, СОУЭ, консолью управления СОУЭ.

Системы видеонаблюдения.

Они же системы охранного телевидения. Оснащение любого объекта системой видеонаблюдения в первую очередь предполагает проведение обследования с целью выявления ответственных зон контроля. Видеонаблюдением в обязательном порядке оснащаются:

- внешний периметр объекта или территории, количество и расположение видеокамер определяется с учётом технических характеристик камер (фокусное расстояние, угол раскрытия, эффективная дальность, наличие и эффективная дальность подсветки), конфигурации периметра для исключения появления «мёртвых зон», наличия освещения для исключения засветки камер в ночное время;

- въездные ворота, калитки, двери во внешнем ограждении;

- входы (выходы) в здание, в том числе эвакуационные;

- стоянки для автотранспорта, погрузочные площадки;

- территория, прилегающая к зданию;

- входные группы, вестибюли;

- места с массовым пребыванием людей (коридоры, лестничные марши);

- спуски в подвалы, выходы на чердаки, крыши;

- для первой категории объекта дополнительно оборудуются потенциально опасные участки и критические элементы, кроме того, для зон прохода и проезда видеокамеры должны обеспечивать распознавание и идентификацию.

Система видеонаблюдения с учетом количества устанавливаемых камер и мест их размещения должна обеспечивать непрерывное видеонаблюдение потенциально опасных участков и критических элементов объекта (территории), архивирование и хранение данных в течение 1 месяца. При расчете дискового пространства лучше учитывать, что видеосигнал записывается круглосуточно. Камеры периметра, входов-выходов, территории должны писать происходящее в круглосуточном режиме, поток с внутренних камер можно писать по детекции, как правило, внутреннее освещение на объектах позволяет обеспечить оптимальную работу алгоритма записи по движению, и в большинстве случаев в ночное время движения внутри знания нет. Кроме того, это позволит увеличить глубину архива.

Системы охранной сигнализации.

Система охранной сигнализации периметра должна обеспечивать контроль проникновения на территорию через ограждение и перемещения по территории. Обычно это оптико-электронные извещатели, «на движение».

На объекте в обязательном порядке системой охранной сигнализации оснащаются все помещения, прилегающие к внешним стенам здания, или имеющие выходы из здания, первого этажа и подвала, цокольного этажа при наличии, чердаков, выходов на крыши. В зависимости от конфигурации здания, может появиться необходимость защиты второго этажа и отдельных помещений этажей выше (при наличии пожарных лестниц, пристроев). Система охранной сигнализации объекта строится в два рубежа. Первый рубеж – окна, внешние двери, внешние стены при необходимости. Для дверей достаточно магнитоконтактных извещателей на открывание, окна защищаются магнитоконтактными извещателями на открывание (по одному на каждую открываемую створку) и акустическими извещателями «на разбитие». Для стен при необходимости (особо важные помещения) используются акустические поверхностные извещатели для оповещения о попытках пролома. Второй рубеж – сами помещения, оборудуются объемными ИК извещателями «на движение». Кроме того, желательно важные помещения защищать дополнительно: ИК извещатели в коридорах перед помещениями, магнитоконтактные извещатели на входных дверях.

Системы контроля и управления доступом.

В первую очередь задача таких систем – не допустить беспрепятственное проникновение посторонних на объект или территорию. Вторая задача – предотвращение несанкционированного доступа в защищаемые помещения. Учет рабочего времени, контроль за перемещением – функции дополнительные. Для удобства желательно для нескольких объектов и территорий систему строить единообразную, с понятным набором идентификаторов, с возможностью управления из одной точки.

Для обеспечения функционала СКУД двери входов в здание оснащаются электромагнитными замками, центральные входы – турникетами и калитками. Двери внутренних помещений могут оснащаться как электромагнитными, так и электромеханическими замками.

Для въездов на территорию как правило устанавливаются автоматические шлагбаумы, управление которыми осуществляется как в ручном режиме, так и автоматически. С учетом

первой категории объектов и территорий въезды должны оснащаться воротами с жестко фиксируемыми створками. Это или распашные ворота с ригелями, или откатные ворота.

Идентификация персонала и обучающихся может осуществляться разными способами. Это карты доступа, брелки, устройства биометрии (отпечатки пальцев, лицо), программные алгоритмы по распознаванию биометрии.

Все системы должны иметь независимое резервируемое электропитание.

Все указанные системы подлежат предварительному проектированию. Это связано с необходимостью вдумчивого обследования объектов и территорий с учетом их особенностей, наличия грамотных специалистов для определения технических решений. Желательно проектирование систем вести комплексно, т.к. во многих случаях работа систем под управлением одной программной оболочки позволяет более оперативно реагировать на тревоги и происшествия. Кроме того, сопряжение систем позволяет оперативно принимать решения на программном уровне. Сопряжение СКУД и АПС позволяет обеспечить беспрепятственную эвакуацию при срабатывании пожарной сигнализации. Сопряжение СОТС и СВН – получение оперативной картинки с камеры при срабатывании датчика в зоне контроля камеры. Сопряжение СКУД и СВН – работу алгоритмов доступа по биометрии, доступа автомобилей по государственному номеру.